

FILED
RICHARD M. NAGEL
CLERK OF COURT

17 APR 14 PM 3:32

U.S. DISTRICT COURT
SOUTHERN DIST OHIO
WEST DIV CINCINNATI

UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
WESTERN DIVISION

**IN RE APPLICATION OF THE UNITED
STATES OF AMERICA FOR AN ORDER
AUTHORIZING THE INSTALLATION
AND USE OF PEN REGISTERS AND
TRAP AND TRACE DEVICES**

CASE NO.

1:17 MJ - 240

A P P L I C A T I O N

(UNDER SEAL)

The United States of America, moving by and through AUSA Karl P. Kadon, its undersigned counsel, respectfully submits under seal this *ex parte* Application for an order pursuant to 18 U.S.C §§ 3122 and 3123, authorizing the installation and use of pen registers and trap and trace devices (“pen-trap devices”) to record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the cellular telephone number **513-485-4751 (Subject Telephone 2, ST2)**, described in Attachment A. In support of this Application, the United States asserts:

1. This is an Application, made under 18 U.S.C. § 3122(a)(1), for an order under 18 U.S.C. § 3123 authorizing the installation and use of a pen register and a trap and trace device.
2. Such an Application must include three elements: (1) “the identity of the attorney for the Government or the State law enforcement or investigative officer making the Application”; (2) “the identity of the law enforcement agency conducting the investigation”; and (3) “a certification by the applicant that the information likely to be obtained is relevant to an ongoing criminal investigation being conducted by that agency.” 18 U.S.C. § 3122(b).
3. The undersigned applicant is an “attorney for the government” as defined in Rule 1(b)(1) of the Federal Rules of Criminal Procedure.

4. The law enforcement agency conducting the investigation is the Federal Bureau of Investigation (FBI).

5. The applicant hereby certifies that the information likely to be obtained by the requested pen-trap devices is relevant to an ongoing criminal investigation being conducted by the FBI into a money laundering organization, where an unknown subject is utilizing **Subject Telephone 2**, in connection with possible violations of Title 18, United States Code, Section 1956.

6. The applicant understands that the FBI and the United States Attorney's Office are directed to comply with the limitations set forth in 18 U.S.C. § 3123(c).

7. This Court is a "court of competent jurisdiction" under 18 U.S.C. § 3122(a)(2) because it "has jurisdiction over the offense being investigated," 18 U.S.C. § 3127(2)(A)(i).

8. Other than the three elements described above, federal law does not require that an Application for an order authorizing the installation and use of a pen register and a trap and trace device specify any facts. The following additional information is provided to demonstrate that the order requested falls within this Court's authority to authorize the installation and use of a pen register or trap and trace device under 18 U.S.C. § 3123(a)(1).

9. A "pen register" is "a device or process which records or decodes dialing, routing, addressing, or signaling information transmitted by an instrument or facility from which a wire or electronic communication is transmitted." 18 U.S.C. § 3127(3). A "trap and trace device" is "a device or process which captures the incoming electronic or other impulses which identify the originating number or other dialing, routing, addressing, and signaling information reasonably likely to identify the source of a wire or electronic communication." 18 U.S.C. § 3127(4).

THE RELEVANT FACTS

10. By way of background, the Federal Bureau of Investigation (herein FBI), New York Division (herein NY), is investigating an intricate money laundering system believed to be

organized by a Mexican drug cartel, known by law enforcement within the United States as the CARTEL JALISCO NEW GENERATION, (herein CJNG). Through the use of their confidential human source (herein NY CHS), a financial broker being used by the CJNG to launder drug proceeds, FBI NY has provided leads to other federal agencies, to include the FBI, Drug Enforcement Administration (DEA) and Homeland Security (HSI), throughout the United States regarding money pickups that have totaled in excess of one million dollars. NY CHS has been determined to be reliable by the FBI NY Agents, because, as stated in more detail below, he/she has provided FBI NY with multiple locations throughout the United States in which money pickups, scheduled by the CJNG, were successfully retrieved by law enforcement. For those reasons Agents believe that the information herein provided by NY CHS regarding criminal activity in the Southern District of Ohio is trustworthy.

11. Agents are aware, based on training and experience, drug traffickers will commonly attempt to launder money by devising schemes in which the money will appear to be the proceeds of lawful business transactions rather than drug trafficking, and can therefore be introduced into traditional financial and banking systems. As previously mentioned, NY CHS, at the direction of FBI NY, has been involved in this process for the CJNG. NY CHS has provided that the CJNG has set up couriers and money pickup points throughout the United States and these couriers are tasked by money brokers with meeting drug customers at predetermined cities, receiving the illicit proceeds, and transporting them to other cities where they are entered into the United States banking system to be laundered and moved to bank accounts owned and operated by the CJNG. Through NY CHS' involvement, FBI NY has been aware of locations and the amounts involved with money pickups throughout the United States and, as stated previously, FBI NY has provided said information to other federal agencies, resulting in additional investigations into local DTO's and/or seized proceeds.

12. Agents are also aware, based on training and experience, that drug traffickers will commonly transport monetary proceeds from narcotics sales separately from narcotics themselves, in order to minimize loss in the event a shipment is interdicted and/or seized by law enforcement. So far, the FBI NY investigation has focused on the laundering of drug proceeds by the CJNG and not the seizure of narcotics. Because of his/her involvement within the money laundering activities of the CJNG, NY CHS knows, and has provided to FBI NY, that the monies being picked up across the United States, as previously stated within this affidavit, are the illicit proceeds from the sale of narcotics.

13. Based on the information disseminated to federal law enforcement agencies within the United States, money pickups have been surveilled and/or seized in Cleveland, Boston, Chicago, Atlanta, Seattle, Toledo and New York. Some of these operations have resulted in arrests of couriers and/or brokers, while others have resulted in local investigations within those cities.

14. In April 2017, based on information provided by NY CHS, a FBI Cincinnati CHS was requested to conduct a money pickup in Ohio from an individual using telephone number **(513)485-4751** (herein **Subject Telephone 2, ST2**). The unknown user was believed to be in possession of \$170,000 in illicit funds.

15. On April 10, 2017 at approximately 10:13 PM, the CHS made a consensually monitored, recorded phone call to **ST2** to schedule the money pickup from the unknown target. The following is a partial transcription of the call:

CHS: You got something for me?

ST2: Yep.

CHS: I'll be coming through tomorrow between...after 12. 1-2 o'clock.

ST2: You said tomorrow?

CHS: Yeah.

ST2: Eww. During the day we don't be so hot we don't be fucking around during the day. It would have to be at night. I was hoping you was here right now.

16. Based on Agents training, experience and knowledge of this investigation, they believe that the CHS was asking the unknown user of **ST2** if he had the \$170,000 "you got something for me?" The unknown user of **ST2** confirmed that he did but stated that he wanted to meet at night because it is "so hot." "Hot" is a common term used to describe an area that is heavily patrolled by police. Later in the conversation the two agree to meet the next day.

17. On April 11, 2017 the CHS had several consensually recorded conversations with **ST2** reference the time and location of the bulk currency pick-up. During one of these conversations the unknown user stated that he would "have his peoples do it." The CHS and **ST2** agreed to meet at the Speedway at North Bend Rd. and Vine St.

18. On April 11, 2017 at approximately 7:45 PM, agents met with the CHS for the purpose of conducting the bulk currency pick up. Agents searched the CHS and the CHS' vehicle for contraband. Nothing was found. The CHS was then provided a digital recorder. The CHS was then sent to the Speedway Gas Station at North Bend and Vine St. The CHS was under constant surveillance. While at the Speedway the CHS had multiple consensually recorded conversations with the **ST2** about the location of the transaction.

19. The following is a partial transcription of a consensually recorded call between the CHS and ST2 that occurred at approximately 8:30 PM:

ST2: Where you at man?

CHS: I'm at the White Castle...I mean at the Speedway. At the Speedway.

ST2: What you driving bra? Hold on bra. Stay on the phone.

20. During this conversation, surveillance units observed a white Honda Accord park next to the CHS' vehicle and the unknown driver threw something into the passenger side of the CHS' vehicle. The unknown subject then immediately left the area driving the Accord.

21. Immediately after the transaction the CHS contacted agents and stated that the transaction was completed. The CHS was followed back to a debriefing location. The CHS was searched for contraband with negative results. Agents recovered a large plastic bag containing a large amount of currency¹. The CHS also provided the digital recorder. During the debrief the CHS confirmed that the unknown driver of the Accord was the subject involved in the transaction.

22. Based on the information provided in the paragraphs above, Agents believe that the unidentified target using **ST2** is involved in the transportation and laundering of drug proceeds for the CJNG.

23. Agents believe the requested information will assist in identifying the user and the location of **ST2**. This could be relevant in: a) locating the source of supply or individuals tied to the source of the supply; b) identifying locations where quantities of money, narcotics and contraband are being stored; and c) identifying other subjects involved in the organization.

24. Based on the information provided in the paragraphs above, Agents believe that the unidentified target using **ST2** is involved in the transportation and laundering of drug proceeds for the CJNG, and is likely located within the Southern District of Ohio. Agents believe that the requested information will assist in identifying the user and location of **ST2**. This could be relevant in: a) locating either the source of supply or individuals tied to the source of supply; b) identifying locations where quantities of money, narcotics and contraband are being stored; and c) identifying the subjects of the unknown organization.

¹ Agents later determined that the bulk cash totaled \$116,190.

25. The conduct being investigated involves use of the cellular telephone number described in Attachment A. To further the investigation, investigators need to obtain the dialing, routing, addressing, and signaling information associated with communications sent to or from that cellular telephone number.

26. The pen-trap devices sought by this Application will record, decode, and/or capture dialing, routing, addressing, and signaling information associated with each communication to or from the cellular telephone number described in Attachment A, including the date, time, and duration of the communication, and those items listed in Attachment B, without geographic limit.

27. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to other kinds of wire and electronic communications, as described below.

28. A cellular telephone, or cell phone, is a mobile device that can transmit and receive both wire and electronic communications. Individuals using cellular telephones contract with cellular service providers, who maintain antenna towers covering specific geographic areas. In order to transmit or receive calls and data, a cellular telephone must send a radio signal to an antenna tower that, in turn, is connected to a cellular service provider's network. A cellular telephone connected to a cellular service provider's network can thus act much like a traditional landline telephone and a computer. This Application seeks both traditional telephone calling data (i.e., telephone numbers dialed and dialing the target device), as well as data related to the dialing, routing, addressing and signaling of electronic communications sent to and from the target device.

29. In addition to a unique telephone number, each cellular telephone has one or more unique identifiers embedded inside it. Depending upon the cellular network and the device, the embedded unique identifiers for a cellular telephone could take several different forms, including

an Electronic Serial Number (“ESN”), a Mobile Electronic Identity Number (“MEID”), a Mobile Identification Number (“MIN”), a Subscriber Identity Module (“SIM”), an International Mobile Subscriber Identifier (“IMSI”), a Mobile Subscriber Integrated Services Digital Network Number (“MSISDN”), or an International Mobile Station Equipment Identity (“IMEI”). When a cellular telephone connects to a cellular antenna or tower, it reveals its embedded unique identifiers to the cellular antenna or tower, and the cellular antenna or tower receives and forwards those identifiers to the core network as a matter of course. The unique identifiers—as transmitted from a cellular telephone to a cellular network—are similar to telephone numbers in that they are used by the cellular provider to identify, authenticate, and/or route the communications. They can be recorded by pen-trap devices and indicate the identity of the cellular telephone device making the communication without revealing the communication’s content.

30. In addition, a list of incoming and outgoing telephone numbers is generated when a cellular telephone is used to make or receive calls, or to send or receive text messages (which may include photographs, videos, and other data). These telephone numbers can be recorded by pen-trap devices and then used to identify the parties to a communication without revealing the communication’s contents.

ELECTRONIC COMMUNICATIONS

31. The Internet is a global network of computers and other devices. On the Internet, data transferred between devices is not sent as a continuous stream, but rather it is split into discrete packets. Generally, a single communication is sent as a series of data packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains user data. The header contains non-content information such as the packet’s

source and destination Internet Protocol (IP) addresses², source and destination port numbers³, transport protocol⁴, flow label⁵ (when IPv6 applies), and the packet's size⁶. The payload usually includes the content of the transmitted communication – for example, part of the text of an e-mail message or the data that makes up part of an electronic image.

32. Cellular phones can connect to the Internet via the cellular network. They can then be used to browse the World Wide Web, send e-mail messages, and engage in other forms of electronic communications, just like desktop computers. When connecting through the cellular network, Internet communications sent and received by a cellular phone will contain some of the same unique identifiers that identify cellular voice communications, such as an ESN, MEID, MIN, SIM, IMSI, MSISDN, or IMEI. Internet communications sent to and from a cellular phone also contain the header information referenced above in each data packet, such as the source and destination IP addresses and the source and destination port numbers associated with that cellular phone at the specific time of the communication. Each of these unique identifiers can be used to

² A numerical label that identifies the source or terminating device on an IP network transmitting an individual packet associated with a communication.

³ Port numbers of the IP packet uniquely identify different applications or processes running on a single device (the source or destination device) and enable the devices to share a single physical connection to a network. This parameter is also used by communication providers for routing of IP packets when utilizing Network Address Translation (NAT), which is common among cellular telephone providers. The source and destination ports are numerical labels that identify the endpoints at the source and destination devices on an IP network transmitting an individual packet associated with a communication. When combined with the source and destination IP addresses, this routing information identifies the source transmitting an IP packet and the destination receiving the IP packet.

⁴ The transport protocol defines the protocol used in the data portion of the IP packet. One example is the Transport Control Protocol, or TCP, which is one of the core protocols of the Internet Protocol suite. TCP provides reliable, ordered and error-checked delivery of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet.

⁵ The field in the IPv6 header that is used by a source to label packets of a flow to avoid disruption during reassembly. This can facilitate such processes as streaming online video or audio feeds. The flow label can be used to indicate to routers and switches with multiple outbound paths that the listed packets should stay on the same path so that they will not be reordered.

⁶ The field that defines the entire packet size, including header and data, in bytes.

identify devices that are party to a communication without revealing the communication's contents. The IP addresses and port numbers recorded in the headers of data packets also are readily available to the cellular service provider in each and every data packet (if they were not, the packets could not be routed to and from their destinations), and can easily be extracted by a pen register and trap and trace device.

33. On the Internet, IP addresses and port numbers function much like telephone numbers and area codes – often both are necessary to route a communication. Devices directly connected to the Internet are identified by a unique IP address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response. Both the IP address of the requesting device (the source IP address) and the IP address of the receiving device (the destination IP address) are included in specific fields within the header of each packet of data sent over the Internet. Source and destination port numbers are also included in specific fields within the headers of data packets. Sometimes these port numbers identify the type of service that is connected with a communication (for example email or web-browsing), but often they identify a specific device on a private network. In either case, port numbers are used to route data packets either to a specific device or a specific process running on a device. Thus, in both cases, port numbers are used by computers to route data packets to their final destinations.

34. The headers of data packets also contain other dialing, routing, addressing and signaling information. This data includes the transport protocol used (there are several different transport protocols that provide transport of data over networks); the flow label (which helps control the path and order of transmission of packets in certain circumstances - for example the

packets that make up streaming video that must be placed in a certain order once received); and the packet size (used to identify the size of each data packet).

35. Because they are all used to facilitate the routing and transfer of data, and because they do not contain the content of communications, the United States requests that this Court order AT&T to either produce, or assist the United States in obtaining through the installation of a Pen Trap device, the IP addresses, port numbers, transport protocol, flow label and packet size of each data packet sent to and from the target device. See 18 U.S.C. §§ 3122 and 3123.

36. The United States further requests that the Court order AT&T to provide other data related to each data packet sent over the provider's network. These data fields are commonly provided by cellular telephone providers pursuant to industry standards adopted under the Communications Assistance for Law Enforcement Act (CALEA). See 47 U.S.C. § 1006. They include: the Case Identification (or Case ID), which is a unique identifier used by law enforcement and the provider to identify the case to which the data pertains; the Intercept Access Point System Identification (IAP System ID), which identifies the network equipment responsible for isolating the targeted information; the Timestamp, which identifies the date and time that the event was detected; and the Correlation Number, which provides a unique identifier for the call data that is used to correlate the communication identifying information with the communication content.

GOVERNMENT REQUESTS

37. For the reasons stated above, the United States requests that the Court enter an Order authorizing the installation and use of pen-trap devices to record, decode, and/or capture the dialing, routing, addressing, and signaling information described above for each communication to or from the cellular telephone number described in Attachment A, to include the date, time, and duration of the communication, and those items listed in Attachment B, without geographic limit.

The United States does not request and does not seek to obtain the contents of any communications, as defined in 18 U.S.C. § 2510(8).

38. Based on the specific and articulable facts set forth above, pursuant to Title 18, United States Code, Sections 2703(c)(1)(B), 2703(c)(2) and 2703(d), the United States requests that AT&T be ordered to supply subscriber information (including the names and addresses of the subscriber, whether listed or unlisted, billing information, payment information, subscriber date of birth, subscriber driver license number, subscriber social security number, equipment information, shipment information, call detail records, information related to calls made via direct connect features, calls to destination search (or “reverse dumps”), and periods of telephone activation) for all numbers dialed or connections made to and from the cellular telephone number described in Attachment A captured by the pen register or trap and trace devices on the cellular telephone number described in Attachment A.

39. The United States further requests that the Court authorize the foregoing installation and use for a period of sixty (60) days from the date of the Court’s Order, pursuant to 18 U.S.C. § 3123(c)(1).

40. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that the Court order AT&T and any other person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of this Order to furnish, upon service of the Order, information, facilities, and technical assistance necessary to install the pen-trap devices, including installation and operation of the pen-trap devices unobtrusively and with minimum disruption of normal service. Any entity providing such assistance shall be reasonably compensated by the FBI, pursuant to 18 U.S.C. § 3124(c), for reasonable expenses incurred in providing facilities and assistance in furtherance of this Order.

41. If AT&T, or any other relevant provider of electronic communication service to the public, cannot comply with this Court's Order to install the pen-trap devices, the United States requests authorization to install and use its own pen register and trap and trace devices on the data network of AT&T, or any other relevant provider of electronic communication service to the public, pursuant to 18 U.S.C. § 3123(a)(3)(A).

42. The United States further requests, pursuant to 18 U.S.C. §§ 3123(b)(2) and 3124(a)-(b), that the Court order AT&T and any other person or entity providing wire or electronic communication service in the United States whose assistance may facilitate execution of this Order, to furnish immediate technical assistance to the FBI to accomplish the interception of all of the dialing, routing, addressing, and signaling information for all data packets associated with each communication to or from the target device, including the date, time and duration of the communication; and to deliver all such intercepted dialing, routing, addressing, and signaling information, securely and reliably and in a format that allows the information to be understood by the applicant. In particular, the United States requests that AT&T and any other person or entity providing wire or electronic communication service in the United States shall provide the following:

- Any requested technical documentation and necessary assistance to enable the FBI to ascertain the meaning and significance of data in the delivery; to facilitate breaking down the information into distinct identifiable fields; and to address deficiencies and preferences with formats.
- A designated technical representative(s)/engineer(s) who will coordinate efforts with and have the authority to provide the FBI's technical staff the necessary information and technical assistance, including direct access to the network facilities used or controlled by or on behalf of the FBI, and any other person or

entity providing wire or electronic communication service in the United States to the target device, for purposes of testing, evaluation and implementation of the technical means necessary to accomplish the authorized pen register and a trap and trace device or process.

43. The United States further requests that the Court order AT&T and any other person or entity whose assistance may facilitate execution of this Order to notify the applicant and the FBI of any changes relating to the cellular telephone number described in Attachment A, including changes to the International Mobile Subscriber Identifier (“IMSI”), and/or the International Mobile Station Equipment Identity (“IMEI”) to include changes to subscriber information; and to provide prior notice to the applicant and the FBI before terminating or changing service to the cellular telephone number.

44. The United States further requests that the Court order that the FBI and the applicant have access to the information collected by the pen-trap devices as soon as practicable, twenty-four hours per day, or at such other times as may be acceptable to them, for the duration of the Order.

45. The United States further requests, pursuant to 18 U.S.C. § 3123(d)(2), that the Court order AT&T and any other person or entity whose assistance facilitates execution of this Order, and their agents and employees, not to disclose in any manner, directly or indirectly, by any action or inaction, the existence of this Application and Order, the resulting pen-trap devices, or this investigation, unless and until authorized by this Court, except that AT&T may disclose this Order to an attorney for AT&T for the purpose of receiving legal advice.

46. The United States further requests that this Application and any resulting Order be sealed until otherwise ordered by the Court, pursuant to 18 U.S.C. § 3123(d)(1).

47. The United States further requests that the Clerk of the Court provide the United States Attorney's Office with three certified copies of this Application and Order, and provide copies of this Order to the FBI and AT&T upon request.

48. The foregoing is based on information provided to me in my official capacity by agents of the FBI.

I declare under penalty of perjury that the foregoing is true and correct.

Executed on this 14th day of April 2017.

Respectfully submitted,

BENJAMIN C. GLASSMAN
United States Attorney

s/Karl P. Kadon

KARL P. KADON (0009324)
Assistant United States Attorney
221 East Fourth Street, Suite 400
Cincinnati, Ohio 45202
Office: (513) 684-3711
Fax: (513) 684-2047
E-mail: Karl.Kadon@usdoj.gov